Transportation Worker Identification Credential (TWIC)

Stakeholder Brief

Transportation Security Administration

TWIC Program

Vision

Improve security by establishing a system-wide common credential, used across all transportation modes, for all personnel requiring unescorted physical and/or logical access to secure areas of the transportation system.

Goals

- Improve security
- Enhance commerce
- Protect personal privacy

Transportation Security Administration

Related Legislation

USA PATRIOT Act of 2001

Requires states to conduct background checks through the Attorney General and TSA before issuing licenses to individuals to transport hazardous materials in commerce.

Aviation and Transportation Security Act of 2001 (ATSA)

Grants the TSA Administrator broad authority for transportation security; requires TSA to ensure the adequacy of security measures at airports; directs strengthened access control points in airport secured areas; and, requires TSA to consider the use of biometric, or similar technologies, to identify individuals employed at airports.

Maritime Transportation Security Act of 2002 (MTSA)

Requires the issuance of biometric transportation security cards and the completion of background checks for entry to any secure area of a vessel or facility.

TWIC Threat Mitigation Goals

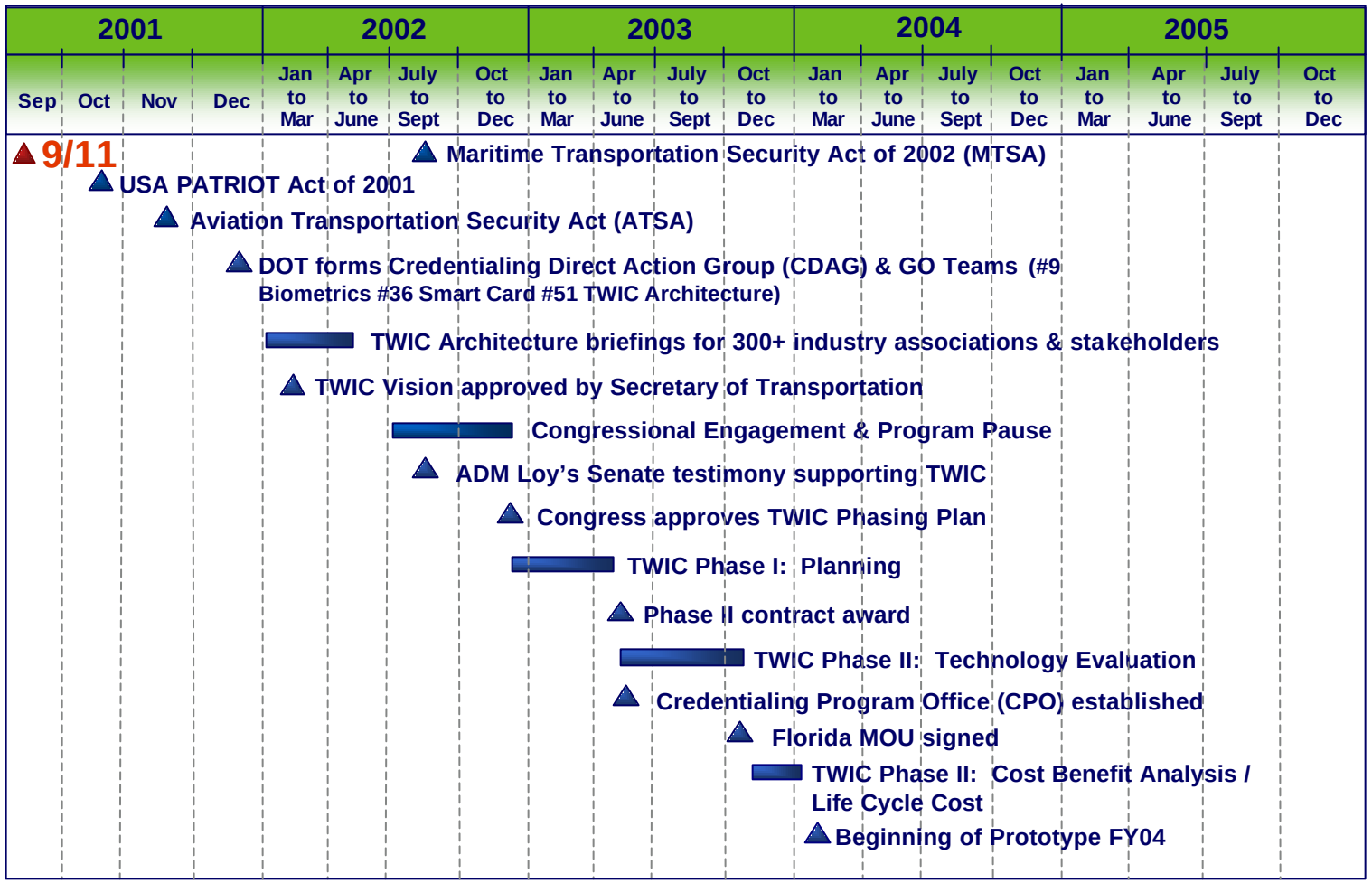
- **Uniformly and consistently ascertain identities**
  - The claimed identity of persons accessing secure areas are not uniformly and consistently verified. Need to prevent persons claiming a false identity from accessing secure areas.

- **Uniformly and consistently match an individual to a valid credential and background check**
  - The performance of this task varies among sites and is non-existent at some. Lack of biometric features on credentials allows use by unauthorized individuals.

- **Uniformly and consistently conduct access threat assessment**
  - The revocation of access privileges is not, and cannot, be consistently accomplished without a uniform process.

- **Provide a tamper-resistant credential**
  - The tamper-resistance of identity credentials varies widely. Credentials may be compromised to permit access by unauthorized individuals.

TWIC Program Timeline



Transportation Security Administration

Potential TWIC Population*

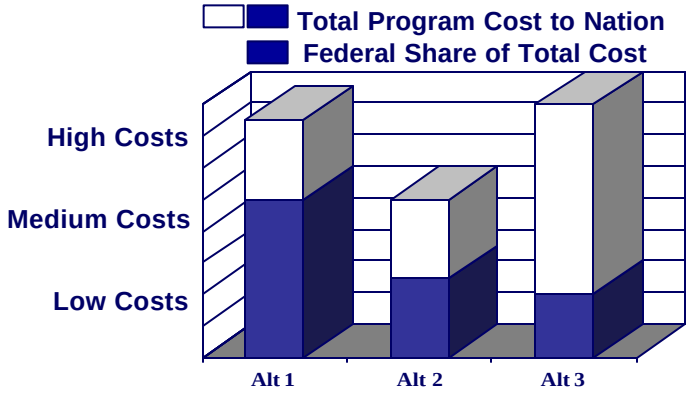
Category	*Anticipated Population*	*Legislative Basis*
Aviation	1,100,000	ATSA
Maritime	1,100,000	MTSA
HAZMAT (CDL)	4,000,000	USA PATRIOT
Other (Mass Transit, Pipeline, Highway, etc.)	5,800,000	USA PATRIOT
Total	12,000,000	

*Source: TWIC Business Case

Transportation Security Administration

Funding Alternatives Analysis

Conducting evaluation of Alternative 2 based on Alternatives Analysis and Balanced Scorecard results.



Alternative 1:
Federal Implementation and Funding

- Common infrastructure
- Matches individual with credential technology
- Centralized control of implementation

- High system replacement costs
- Public perception / privacy concerns
- Potential impact on commerce

Alternative 2:
Federally led Public / Private Partnership

- **Common infrastructure**
- **Matches individual with credential technology**
- **Leverage existing systems**
- **Options for shared cost**

- **Requires local commitment to Public / Private Partnership**

INVESTIGATE

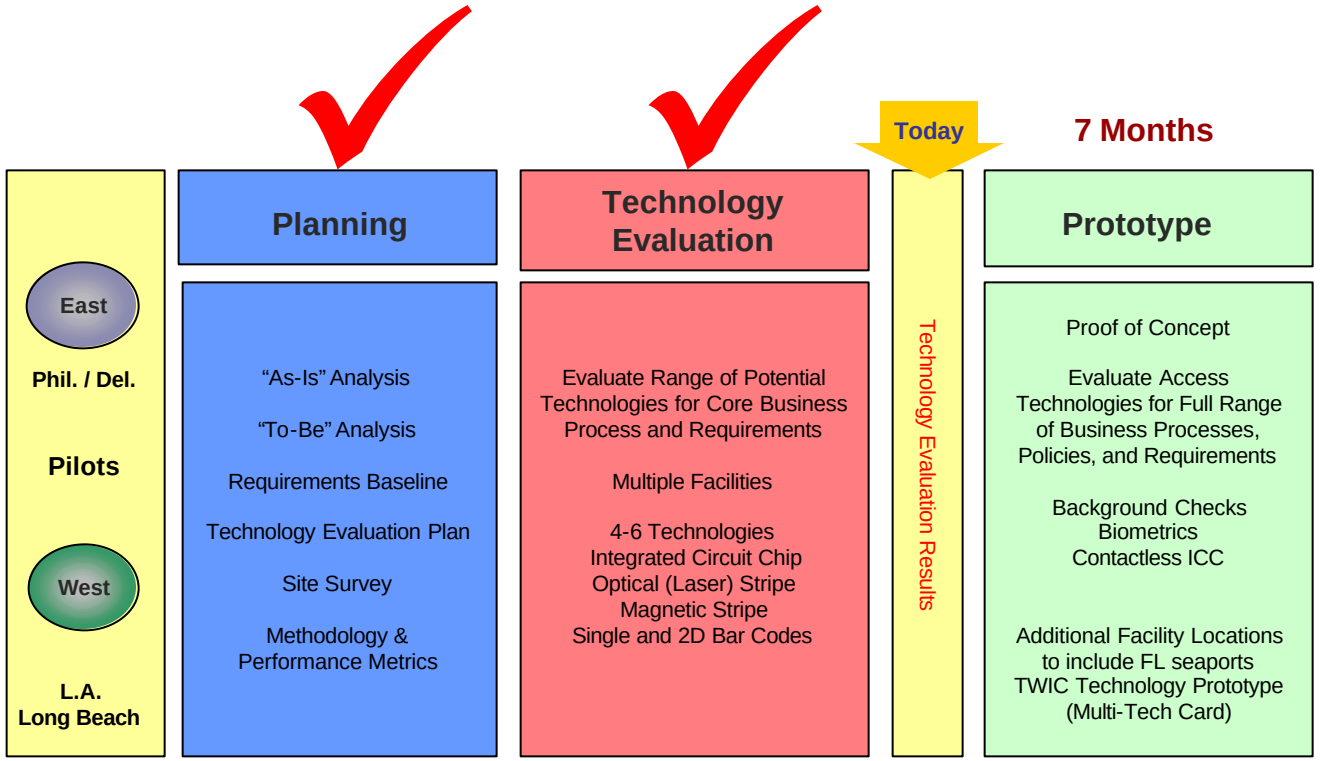
Alternative 3:
Federal Regulation / Local Implementation and Funding

- Stakeholder independence
- Matches individual with credential technology
- Local acceptance

- Divergent to interoperability goal
- Requires 100% local implementation, design, and execution
- Lack of economy of scale

Transportation Security Administration

TWIC Program Status



- Planning and Technology Evaluation Phases are complete.
- Results are being analyzed.
- Prototype Phase planning is being finalized.

Transportation Security Administration

Concurrent Activities

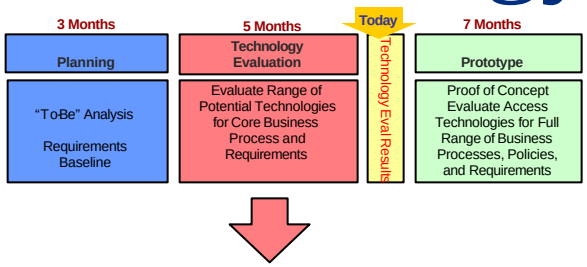
*Systems Development Life Cycle

**Identification Management System

***Law Enforcement Officer

Transportation Security Administration

Technology Evaluation Review



- **Tested 5 card-based technologies at 12 transportation facilities in 2 regions:**
  - Integrated Circuit Chip
  - 2-D Barcode
  - Magnetic Stripe
  - Optical (Laser) Memory Stripe
  - Linear Bar Code
- **Issued cards to a broad range of transportation workers:**
  - Union workers (ILWU, AFL-CIO, etc.)
  - Independent truck drivers
  - Crane operators
  - Non-union workers, managers, owners
  - Security guards
  - Pipeline workers
  - Airline mechanics
  - Railroad employees
  - Tug boat crews
- **Evaluated the technologies in many types of physical & logical access transactions:**
  - Vehicle gates
  - Staffed guard stations
  - IT system sign-on
  - Truck multi-lanes
  - Unattended building entrances
  - Internal building doors
  - Unattended gates
  - High volume pedestrian turnstile
  - Parking garage exit points
- **Evaluated central card production:**
  - Produced the final increment of cards for the West Coast region at the DHS facility in Corbin KY
- **Operated enrollment centers, local issuance, help desk, and card management systems to support phase requirements.**

Transportation Security Administration

Technology Evaluation Test Plan

Purpose *Evaluate multiple access control technologies for core business processes and requirements.*

East Coast Sites

West Coast Sites

		Port of Wilmington, DE	Packer Avenue Terminal, PA	Beckett Street Terminal, NJ	APL Terminal, CA	Long Beach Container Terminal, CA	Crowley Marine Services, CA	Delaware River & Bay Maritime Exch, PA	Port of Long Beach, CA	Port of Los Angeles, CA	Conoco Phillips Oil Refinery, PA	PHL Airport, PA	ICTF Union Pacific Rail, CA
	Enrollment	X	X	X	X	X	X	X	X	X	X	X	X
Access Control Technologies	Optical (Laser) Memory Stripe			X				X	X	X	X		
	ICC	X	X		X	X		X		X			
	Bar Code (2D)					X					X		
	Bar Code (3x9)	X											
	Magnetic Stripe	X					X	X	X			X	X

Transportation Security Administration

Technology Evaluation Review

Access Control Types	Card Technologies				
	Magnetic Stripe	**Linear Bar Code**	**2-D Bar Code**	**ICC**	**Optical (Laser) Stripe**
Physical Staffed (Fixed) PC	✓	✓	✓	✓	✓
Physical Staffed (Mobile) Handheld Tablet and Reader	X	X	X	✓	X
Physical Automated (Un-staffed) / Mounted Reader / Turnstile/ Door	✓	X	X	✓	X
Logical (PC or Laptop)	X	X	X	✓	X

✓ **indicates that the technology passed the initial survey and was evaluated during the Technology Evaluation Phase.**

X **indicates that the technology failed the initial survey, the capability is not COTS, and was not evaluated.**

The following were the selection factors:

- Hardware is in production and is readily available.
- Software is commercially available.
- Technology provides a measurable level of security.
- Physical features and form factors are ergonomically acceptable for operational environment.
- Solution is available for deployment within required timeframe.

Transportation Security Administration

Technology Evaluation Results

Card Technology Capabilities Matrix
Strength / Weakness Analysis

Card Technology Attributes	Magnetic Stripe	Linear Bar Code	2-D Bar Code	IC Chip	Optical Stripe
Physical Access Usage	Strong	Weak	Weak	Strong	Weak
Logical Access Usage	Weak	Weak	Weak	Strong	Weak
Capacity	Weak	Weak	Moderate	Strong	Strong
Security	Moderate	Weak	Weak	Strong	Moderate
Read / Write Capability	Moderate	Weak	Weak	Strong	Moderate
Processing Capability	Weak	Weak	Weak	Strong	Weak
Reader Technology	Moderate	Strong	Strong	Moderate	Moderate
Backward Compatibility	Strong	Weak	Weak	Strong	Weak
Relative Cost for Access Transaction	Moderate	N/A	N/A	Moderate	Expensive

- Integrated Circuit Chip (ICC) Smart Card is the most appropriate technology for the TWIC requirements, providing a commercially available, secure solution for both physical and logical access.
- Magnetic Stripe has deficiencies in physical access security and logical access capability, but is widely used and should be included so that legacy systems at the facility level can be upgraded.
- Optical stripe has deficiencies in physical access security and logical access capability, and appropriate software and peripheral equipment is not commercially available.
- Linear and 2-D Barcodes have limited physical access capability and do not provide adequate security features.

Transportation Security Administration

Prototype System Overview

- Leverage current East and West Region Pilots
- Leverage Florida Uniform Port Access Credential (FUPAC) system
- Support other high priority pilot initiatives

Port

Airport

Port

Los Angeles Long Beach

Enrollment

Delaware River and Bay

Enrollment

Port

Airport

Port

IDMS*

Background Checks

Threat List

Hotlist Bio Match

DHS & TSA HQ

Enrollment

Florida

Enrollment

TWIC Prototype Card Production Center

DHS/ TSA

Port A

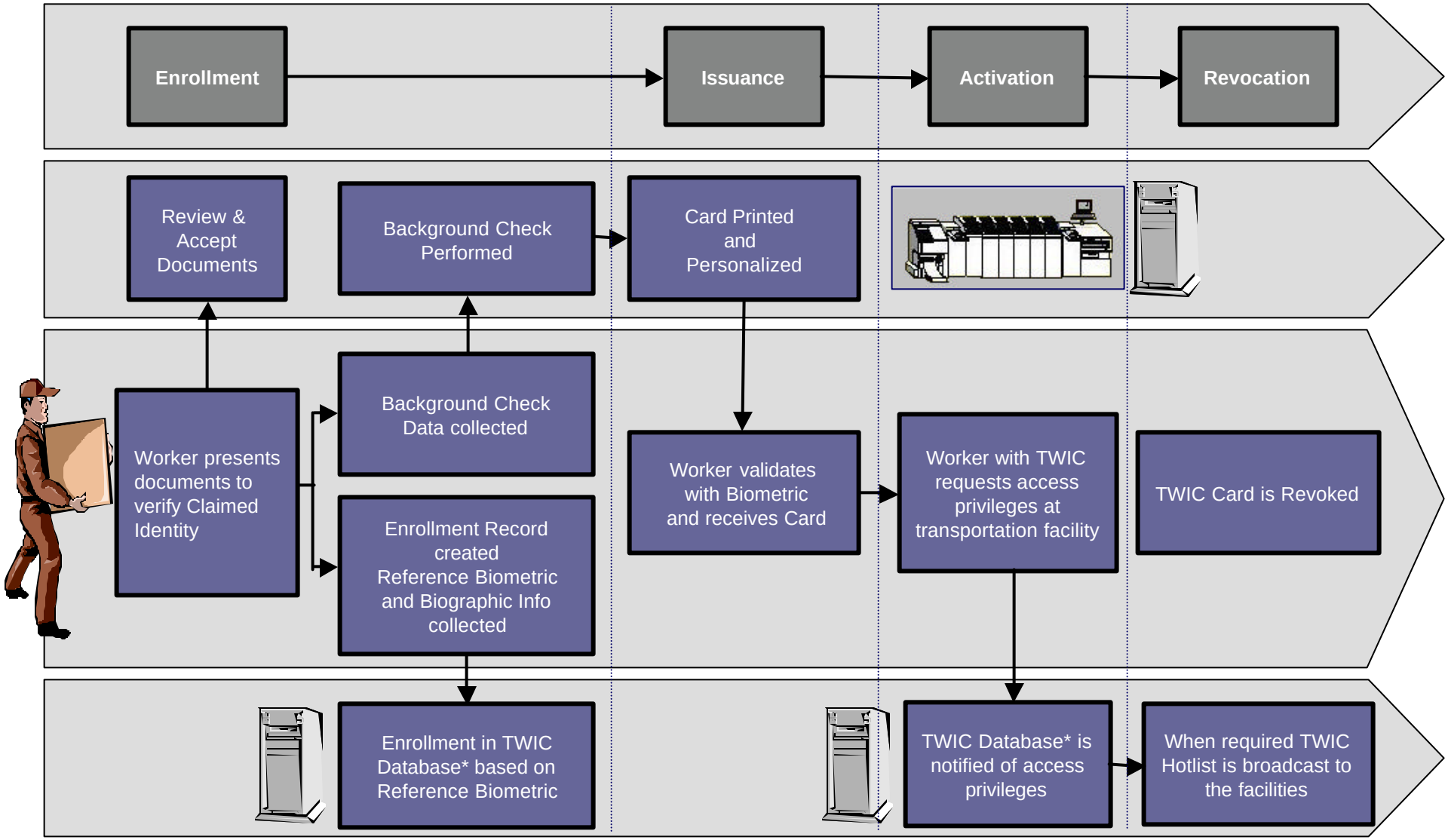
Port B

Port C

*Identity Management System

Transportation Security Administration

Overview of TWIC Business Processes



*** TWIC will evaluate various Federal, State, and Local Database Options**

Transportation Security Administration

Prototype Test Plan

Illustrative

Purpose: *Broaden evaluation using multiple technologies over the full range of business processes and requirements.*

- East Coast Sites
- West Coast Sites
- Florida Seaports

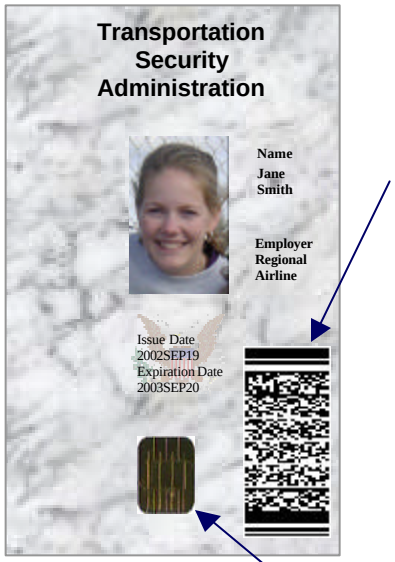
		Maritime									HQ				Pipeline		Air		Rail	Other	
		Port of Wilmington, DE	Packer Avenue Terminal, PA	Penns Terminal, PA	Beckett Street Terminal, NJ	APL Terminal, CA	Maersk Terminal, CA	LBCT Terminal, CA	Crowley Marine, CA	14 Florida Ports	Delaware River & Bay Maritime Exch, PA	Port HQ Long Beach, CA	DHS	Port HQ Los Angeles, CA	BP Refinery, CA	Conoco Phillips Oil Refinery, PA	PHL Airport, PA	LAX Airport, CA	Union Pacific Rail ITCF, CA	Customs House, PA	ILWU Union Hall, CA
Business Processes	TWIC Multi-Application / Multi-Technology Solution	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X
	Contactless	X									X	X		X			X				
	Biometrics	X			X					X	X	X		X				X	X		

Card Architecture

Illustrative of Surface Technologies

FRONT

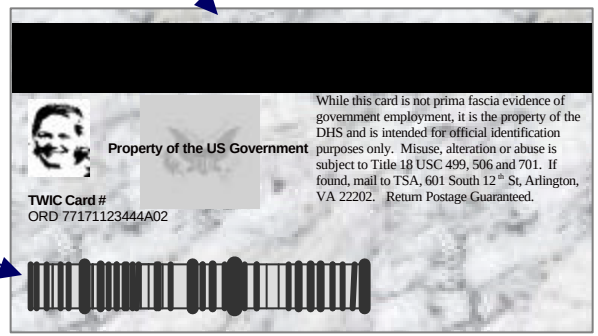
BACK



2D Bar Code

ICC Chip

Magnetic Stripe



Linear Bar Code

Transportation Security Administration

Privacy Considerations - Guiding Principles

- **Minimum Data**: Collect and retain only data that is absolutely necessary
- **Limit Use**: Use the data only for the purpose for which it was collected
- **Data Quality**: Ensure data maintained is accurate, complete, current, and relevant
- **Data Security**: Secure and protect data from unauthorized use (physical and cyber)
- **Accountability**: Use internal controls to protect the privacy of individual information
- **Procedural Safeguards**: Use logical access authentication for those who have access to any part of data. Data will be filtered to preclude access by unauthorized individuals.

Transportation Security Administration

Beyond the Scope of TWIC

- **Possession of a TWIC does not automatically grant the holder access to secure areas.**
  - Only facilities grant access. Facilities have complete control over who is granted access to secure areas, and what level of access is granted.

- **The TWIC program will not develop site-specific secure area definitions.**
  - The TWIC regulations will point to the definitions of “secure areas” as determined in national security plans, regulations or by statute.

- **The TWIC program does not prevent facilities from specifying additional access requirements.**
  - Facilities may require background check, access procedures, or credentials beyond those provided by TWIC.

Conclusion

TWIC Program Benefits

Improves Security

- Reduced risk of fraudulent or altered credentials
- Biometrics used for secure, positive match of individual to authorized access level and clearances
- Ability to interface and communicate with other federal, local, and state agencies
- Ability to disseminate “threat alerts” throughout a nationally integrated system

Protects Individual Privacy

- Collection of minimum data elements
- Secure record control system and network
- Employs advanced information technology to protect personal information
- System-wide encryption implementation at the end of the implementation phase

Enhances Commerce

- Increases process speed and efficiency
- Enables improved management and utilization of resources
- Expanded e-government potential
- Public – private partnership
- Economies of scale purchasing
- Eliminates need for redundant credentials and background investigations
- Leverages current security investment and legacy systems

Transportation Security Administration

Contact Information

For additional information, please e-mail us at

Credentialing@tsa.dot.gov

Transportation Security Administration

Transportation Security Administration